

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 11205388 A

(43) Date of publication of application: 30.07.99

(51) Int. Cl

**H04L 12/66
G09C 1/00
H04L 9/32
H04L 12/56**

(21) Application number: 10007682

(22) Date of filing: 19.01.98

(71) Applicant: HITACHI LTD

(72) Inventor: HASHIMOTO KAZUO
NISHIKADO TAKASHI
KAWAGUCHI KENJI
OTA MASATAKA

**(54) PACKET FILTER, AUTHENTICATION SERVER,
PACKET FILTERING METHOD AND STORAGE
MEDIUM**

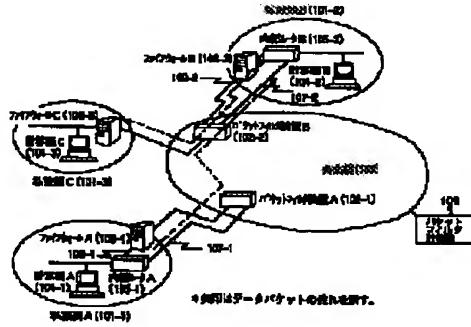
packet is sent to the firewall 106.

COPYRIGHT: (C)1999,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide the high speed packet filtering system that prevents a 3rd party from illegally intruding the internet VPN.

SOLUTION: The system is provided with a direct path connecting directly with a private network from the packet filter system 102, and a fire wall path via a firewall 106. The packet filter system 102 adds predetermined authentication information to a data packet received from a private network and sends the resulting packet to a public network and also sends the data packet received from the firewall 106 to the public network. The system 102 discriminates whether or not the data packet received from the public network is a data packet to which the authentication information is added. When the data packet is a packet to which the authentication information is added, the authentication information is eliminated from the packet and the resulting data packet is sent to the private network. When the data packet is not a packet to which the authentication information is added, the resulting data



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-205388

(43)公開日 平成11年(1999)7月30日

(51)Int.Cl.⁶
H 04 L 12/66
G 09 C 1/00
H 04 L 9/32
12/56

識別記号
6 6 0

F I
H 04 L 11/20
G 09 C 1/00
H 04 L 9/00
11/20

B
6 6 0 E
6 7 5 A
1 0 2 A

審査請求 未請求 請求項の数13 O.L (全13頁)

(21)出願番号 特願平10-7682

(22)出願日 平成10年(1998)1月19日

(71)出願人 000005108

株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72)発明者 楠本 和夫
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 西門 隆
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 川口 研治
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74)代理人 弁理士 富田 和子

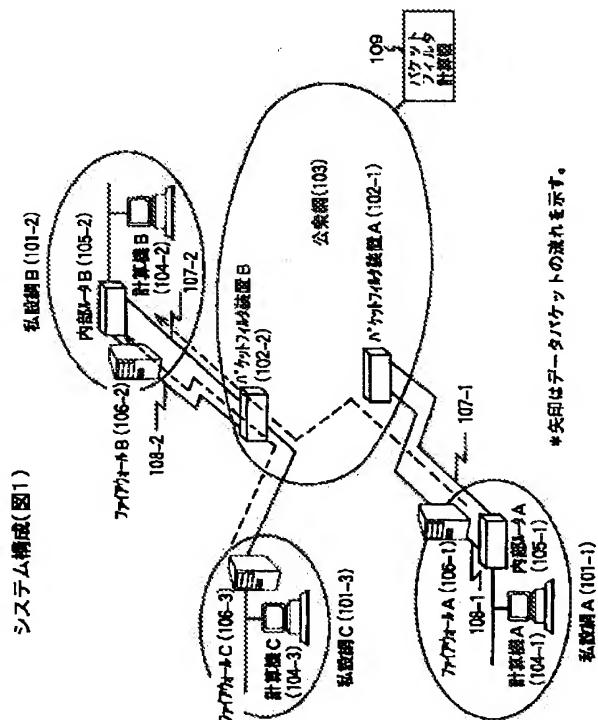
最終頁に続く

(54)【発明の名称】 パケットフィルタ装置、認証サーバ、パケットフィルタリング方法及び記憶媒体

(57)【要約】

【課題】インターネットVPNにおいて、第三者がVPN内へ不正に侵入することを防ぎ、高速なパケットフィルタリング装置を提供する。

【解決手段】パケットフィルタ装置から直接私設網に接続された直結経路と、ファイアウォールを介したファイアウォール経路とを設けておく。パケットフィルタ装置は、私設網から受信したデータパケットにあらかじめ定めた認証情報を付加して公衆網に送信し、ファイアウォールから受信したデータパケットを公衆網に送信する。また、公衆網から受信したデータパケットが、認証情報が付加されたデータパケットであるかないかを判断し、認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、私設網へ当該データパケットを送信する。前記認証情報が付加されたデータパケットでなければ前記ファイアウォールへ当該データパケットを送信する。



【特許請求の範囲】

【請求項1】ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置であって、前記公衆網に接続される公衆接続部と、前記私設網に直接接続される私設接続部と、前記ファイアウォールに接続されるファイアウォール接続部と、

前記私設接続部で受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆接続部から前記公衆網に送信し、前記ファイアウォール接続部で受信したデータパケットを前記公衆接続部から前記公衆網に送信するパケット転送手段と、前記公衆接続部で受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断し、前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設接続部から当該データパケットを送信し、前記認証情報が付加されたデータパケットでなければ前記ファイアウォール接続部から当該データパケットを送信するパケット振り分け手段とを有することを特徴とするパケットフィルタ装置。

【請求項2】請求項1に記載のパケットフィルタ装置において、前記認証情報に対応する認証キー情報を記憶する認証キー記憶手段と、前記認証キー情報を、前記認証キー記憶手段に設定する認証キー設定手段とをさらに有することを特徴とするパケットフィルタ装置。

【請求項3】請求項2に記載のパケットフィルタ装置において、前記パケット転送手段は、前記認証キー記憶手段に記憶する認証キー情報を前記認証情報を作成する作成手段と、前記作成手段により作成された認証情報を前記データパケットのあらかじめ定めた領域に付加する付加手段とを備えることを特徴とするパケットフィルタ装置。

【請求項4】請求項2に記載のパケットフィルタ装置において、前記パケット振り分け手段は、前記データパケットから認証情報を抽出し、当該認証情報が、前記認証キー記憶手段に記憶する認証キー情報をから作成した認証情報と一致するかいかを判断する検査手段と、前記検査手段により、一致する認証情報が付加されたデータパケットであれば、当該認証情報を取り除く削除手段とを備えることを特徴とするパケットフィルタ装置。

【請求項5】請求項1に記載のパケットフィルタ装置において、複数のプライベートネットに対応する前記私設接続部を複数備え、前記パケット転送手段は、前記複数のプライベートネットワークの各々に対応する認証情報を付加し、前記パケット振り分け手段は、前記複数のプライベートネットワークの各々に対応する認証情報から、当該認証情報に対応する前記私設接続部を判断し、対応する私設接続部から当該データパケットを送出することを特徴とするパケットフィルタ装置。

【請求項6】請求項5に記載のパケットフィルタ装置に

おいて、複数のプライベートネットに対応する前記公衆接続部を複数備えることを特徴とするパケットフィルタ装置。

【請求項7】請求項5または6に記載のパケットフィルタ装置において、前記複数のプライベートネットワークの各々に対応する認証情報を対応する認証キー情報を各々記憶する認証キー記憶手段と、前記認証キー情報を各々を、前記認証キー記憶手段に設定する認証キー設定手段とをさらに有することを特徴とするパケットフィルタ装置。

【請求項8】パケットの送信元に従ってパケットを振り分けるパケットフィルタ装置であって、前記送信元からパケットを受信するための第1の接続部と、前記パケットを出力する第2および第3の接続部と、前記第1の接続部で受信したパケットがあらかじめ定めた送信元から送信されたパケットであるかないかを判断し、前記あらかじめ定めた送信元からのパケットであれば、前記第2の接続部から当該データパケットを送信し、前記あらかじめ定めた送信元からのパケットでなければ前記第3の接続部から当該データパケットを送信させるパケット振り分け手段とを有することを特徴とするパケットフィルタ装置。

【請求項9】請求項8に記載のパケットフィルタ装置において、前記第2および第3の接続部は、パケットをさらに受信し、前記第2の接続部で受信したパケットがあらかじめ定めた送信元情報を付加して前記第1の接続部から当該パケットを送信し、前記第3の接続部で受信したパケットはそのまま第1の接続部から送信させるパケット転送手段をさらに有することを特徴とするパケットフィルタ装置。

【請求項10】パケットの送信元に従ってパケットを振り分けるパケットフィルタ装置であって、前記送信元からパケットを受信するための第1の接続部と、前記パケットを出力する第2および第3の接続部と、処理を行うCPUと、前記第1の接続部で受信したパケットがあらかじめ定めた送信元から送信されたパケットであるかないかを判断し、前記あらかじめ定めた送信元からのパケットであれば、前記第2の接続部から当該データパケットを送信し、前記あらかじめ定めた送信元からのパケットでなければ前記第3の接続部から当該データパケットを送信させるためのプログラムを記憶するメモリとを有することを特徴とするパケットフィルタ装置。

【請求項11】私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置に対して、当該パケットフィルタ装置におけるパケット振り分けのための認証キー情報を送信する認証サーバであって、前記パケットフィルタ装置が当該認証サーバへのアクセスが正当であるかないかを判断する判断手段と、前記判断手段により正当と判断されたパケットフィルタ装置に対して前記プライベートネットワー-

クに対応する認証キー情報を送信する送信手段とを備えることを特徴とする認証サーバ。

【請求項12】ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタリング方法であって、前記私設網から受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆網に送信するステップと、前記ファイアウォールから受信したデータパケットを前記公衆網に送信するステップと、前記公衆網から受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断するステップと、前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設網へ当該データパケットを送信するステップと、前記認証情報が付加されたデータパケットでなければ前記ファイアウォールへ当該データパケットを送信するステップとを備えることを特徴とするパケットフィルタリング方法。

【請求項13】請求項12に記載のステップを情報処理装置により実現するためのプログラムを記憶する記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信網間を接続してデータパケットをフィルタリングする技術に係り、特に、アプリケーション毎のチェック機能を有するファイアウォールと連携して高速で且つ安全性の高いパケットフィルタリング方法及びその装置を提供するものである。

【0002】

【従来の技術】近年、公衆網を用いて私設網をそれぞれ接続し、私設網の広域化を実現するインターネットVPN (Virtual Private Network) の構築が盛んになりつつある。私設網を公衆網に接続させる場合、公衆網での盗聴及び不正アクセスにさらされる危険性があり、セキュリティ面で大きな問題点がある。

【0003】このような問題点に対して、各ユーザが、暗号化手段やアクセス制御手段をもつファイアウォールを導入してセキュリティ面でのリスクをできる限り小さくすることが可能である。既に、各社より暗号化手段を備えたファイアウォールが出荷されている。例えば、日経コミュニケーション1996.6.17 Nb.224の86頁～100頁にインターネットVPNが紹介されている。

【0004】このインターネットVPNについて図12を参照して説明する。

【0005】図12において、私設網A101-1と私設網B101-2とは、それぞれの私設網内に設置されたファイアウォールA106-1及びファイアウォールB106-2を介して公衆網103にそれぞれ接続される。ファイアウォールA106-1及びファイアウォールB106-2は、暗号化手段を備える不正アクセスを防ぐためのゲートウェイ装置である。

【0006】例えば、計算機A104-1が計算機B104-2と通信する場合、以下の手順で行われる。

【0007】計算機Aは、計算機Bに対してデータパケットの送信を行う。送信されたデータパケットは、ヘッダ部にあらかじめ定められた送信元アドレス及びポート番号が書かれており、ファイアウォールAで暗号化されて公衆網に送信される。

【0008】暗号化されたデータパケットは、公衆網を介してファイアウォールBに送られる。

【0009】ファイアウォールBでは、データパケットの復号化を行う。また、データパケットのヘッダ部に書かれた送信元アドレス及びポート番号よりアクセス権限をチェックして、アクセス可能な計算機と判断した場合、データパケットを計算機Bに送信する。不正なアクセスと判断した場合、計算機Bにはデータパケットを送らない。

【0010】次に、図13を参照してファイアウォール106の内部構成を説明する。図13に、ファイアウォール106の内部構成図を示す。図13において、ファイアウォール

106は、ネットワークに接続される入出力手段1301、暗号化および復号化を行う暗号化手段1302、不正アクセスを防ぐためのコネクション管理手段1303、及び、アプリケーション毎のアクセスを管理するためのアプリケーション管理手段1304を備える。コネクション管理手段及びアプリケーション管理手段は、参照テーブルとして、アクセス可能な、送信元の計算機のアドレスおよびポート番号を記憶するコネクション管理テーブルA1305、及び、アプリケーションプロトコル毎に定義されたアクセス可能な計算機のアドレスを記憶するコネクション管理テーブルB1306を備えている。

【0011】入出力手段1301は、データパケット1307を通信網からファイアウォール内部に入力し、又、通信網上に出力する手段である。

【0012】暗号化手段1302は、ペイロード1307-2の暗号化、復号化を行う手段である。

【0013】コネクション管理手段1303は、ヘッダ1307-1に書かれたポート番号及び送信元アドレスから、コネクション管理テーブルA1305に書かれたアクセス可能な計算機が否かを判断する手段である。

【0014】アプリケーション管理手段1304は、アプリケーションプロトコル毎に定義されたアクセス制御情報を基づいてアクセス可能な計算機かどうかを判断する手段である。データパケット1307のペイロード1307-2に書かれたアクセス制御情報からコネクション管理テーブルB1306に書かれたアクセス可能な計算機が否かを判断する。なお、アプリケーション管理手段は、アプリケーションプロトコル毎に仕様が異なっており、ファイアウォールがサポートするアプリケーションプロトコルの数だけ備えることができる。

【0015】

【発明が解決しようとする課題】上述した従来技術を用いて、ファイアウォールによるデータパケットの暗号化及びアクセス制御を行うことで公衆網を使ったインターネットVPNを構築することは可能である。しかし、ファイアウォールには、以下に示すような問題がある。

【0016】アプリケーションプロトコル毎にコネクションを管理する方法は、高いセキュリティを確保できる反面、アプリケーションプロトコル毎にそれぞれ異なる対応をしなければならない。通常、複数のアプリケーションが通信網を利用するため、ファイアウォールはそれら全てに対応しなければならず、処理が煩雑になる。結果として、処理時間がかかるてしまう。例えば、前述したインターネットVPNを利用する際に、インターネットVPNに接続されていない計算機とも通信を行う場合には、ファイアウォールでは、インターネットVPNに接続されている計算機であるか、否かに関わらず、前述した、すべてのアプリケーションについてのアクセス権限のチェックを行う。この処理に時間がかかるっている。

【0017】一方、インターネットVPNを、公衆網側でサービスとして提供されることが望まれている。この場合、既存の設備を利用しつつ、新たなサービスを受けられることが望ましい。

【0018】そこで、本発明は、処理速度の高速化を図り、高いセキュリティを確保できるインターネットVPNのサービスを提供するためのパケットフィルタ装置、認証サーバ、パケットフィルタリング方法及び記憶媒体を提供することを目的とする。

【0019】

【課題を解決するための手段】本発明は、処理速度の高速化と、高いセキュリティを確保したインターネットVPNを提供するため、以下の手法を用いる。

【0020】ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置であって、前記公衆網に接続される公衆接続部と、前記私設網に直接接続される私設接続部と、前記ファイアウォールに接続されるファイアウォール接続部と、前記私設接続部で受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆接続部から前記公衆網に送信し、前記ファイアウォール接続部で受信したデータパケットを前記公衆接続部から前記公衆網に送信するパケット転送手段と、前記公衆接続部で受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断し、前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設接続部から当該データパケットを送信し、前記認証情報が付加されたデータパケットでなければ前記ファイアウォール接続部から当該データパケットを送信するパケット振り分け手段とを有する。

【0021】前記認証情報に対応する認証キー情報を記

憶する認証キー記憶手段と、前記認証キー情報を、前記認証キー記憶手段に設定する認証キー設定手段とをさらに有する。前記パケット転送手段は、前記認証キー記憶手段に記憶する認証キー情報から前記認証情報を作成する作成手段と、前記作成手段により作成された認証情報を前記データパケットのあらかじめ定めた領域に付加する付加手段とを備える。

【0022】前記パケット振り分け手段は、前記データパケットから認証情報を抽出し、当該認証情報が、前記認証キー記憶手段に記憶する認証キー情報から作成した認証情報と一致するかいかを判断する検査手段と、前記検査手段により、一致する認証情報が付加されたデータパケットであれば、当該認証情報を取り除く削除手段とを備える。

【0023】複数のプライベートネットに対応する前記私設接続部を複数備え、前記パケット転送手段は、前記複数のプライベートネットワークの各々に対応する認証情報を付加し、前記パケット振り分け手段は、前記複数のプライベートネットワークの各々に対応する認証情報から、当該認証情報に対応する前記私設接続部を判断し、対応する私設接続部から当該データパケットを送出する。また、複数のプライベートネットに対応する前記公衆接続部を複数備えることを特徴とするパケットフィルタ装置。

【0024】前記複数のプライベートネットワークの各々に対応する認証情報に対応する認証キー情報を各々記憶する認証キー記憶手段と、前記認証キー情報の各々を、前記認証キー記憶手段に設定する認証キー設定手段とをさらに有するようにしてもよい。

【0025】また、パケットの送信元に従ってパケットを振り分けるパケットフィルタ装置であって、前記送信元からパケットを受信するための第1の接続部と、前記パケットを出力する第2および第3の接続部と、前記第1の接続部で受信したパケットがあらかじめ定めた送信元から送信されたパケットであるかないかを判断し、前記あらかじめ定めた送信元からのパケットであれば、前記第2の接続部から当該データパケットを送信し、前記あらかじめ定めた送信元からのパケットでなければ前記第3の接続部から当該データパケットを送信させるパケット振り分け手段とを有する。前記第2および第3の接続部は、パケットをさらに受信し、前記第2の接続部で受信したパケットにあらかじめ定めた送信元情報を付加して前記第1の接続部から当該パケットを送信し、前記第3の接続部で受信したパケットはそのまま第1の接続部から送信させるパケット転送手段をさらに有する。

【0026】ハードウエア構成としては、前記送信元からパケットを受信するための第1の接続部と、前記パケットを出力する第2および第3の接続部と、処理を行うCPUと、前記第1の接続部で受信したパケットがあらかじめ定めた送信元から送信されたパケットであるかな

いかを判断し、前記あらかじめ定めた送信元からのパケットであれば、前記第2の接続部から当該データパケットを送信し、前記あらかじめ定めた送信元からのパケットでなければ前記第3の接続部から当該データパケットを送信させるためのプログラムを記憶するメモリとを有する。

【0027】また、私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置に対して、当該パケットフィルタ装置におけるパケット振り分けのための認証キー情報を送信する認証サーバであって、前記パケットフィルタ装置が当該認証サーバへのアクセスが正当であるかないかを判断する判断手段と、前記判断手段により正当と判断されたパケットフィルタ装置に対して前記プライベートネットワークに対応する認証キー情報を送信する送信手段とを備える。

【0028】ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタリング方法であって、前記私設網から受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆網に送信するステップと、前記ファイアウォールから受信したデータパケットを前記公衆網に送信するステップと、前記公衆網から受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断するステップと、前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設網へ当該データパケットを送信するステップと、前記認証情報が付加されたデータパケットでなければ前記ファイアウォールへ当該データパケットを送信するステップとを備える。これらのステップを情報処理装置により実現するためのプログラムは、記憶媒体に記憶しておくことができる。以上の動作により、VPNを構成する私設網間のデータパケットは、セキュリティが保証できる。また、パケットフィルタ装置が付加する認証情報は、アプリケーションプロトコルに係わらず一定であるためハードウェアによる高速化が可能であり、高速なアクセス制御が行える。更に私設網内のあるVVサーバへのアクセスを許す場合や、逆に私設網から公衆網上のVVサーバをアクセスする際等、VPN外の情報処理装置へのアクセスはファイアウォールを経由して行えるので、速度は私設接続部より落ちるが、細やかなセキュリティの実現が可能である。

【0029】なお、公衆網とパケットフィルタ装置の間は一つの回線で接続されるため、専用線と一般公衆線を分けずに一つの回線契約で実現できるという利点もある。

【0030】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態を詳しく説明する。

【0031】図1は、本発明の一実施の形態であるシス

テム構成図を示している。図1において、本システム構成では、私設網A101-1、私設網B101-2及び私設網C101-3が存在する。私設網A及び私設網Bは、公衆網103を介してVPNを構成する私設網の対とし、私設網Cは、公衆網103を介して他の私設網とVPNを構成しない私設網とする。

【0032】公衆網には、私設網A及び私設網BのVPNを構成させるため、パケットフィルタ装置A102-1を設け、私設網Aに接続させる。私設網Bと公衆網との接続点にも同様に、パケットフィルタ装置B102-2を設ける。私設網Cは、他とVPNを構成しないため、パケットフィルタ装置を必要としない。

【0033】私設網Aとパケットフィルタ装置Aとの接続には、二経路を設ける。一経路は、パケットフィルタ装置Aと内部ルータA105-1とを直接接続させる直結経路107-1であり、もう一経路は、ファイアウォールA106-1を経由して内部ルータAに接続させるファイアウォール経路108-1である。計算機A104-1は、内部ルータAに接続される。私設網Bとパケットフィルタ装置Bとの接続方法も、私設網Aとパケットフィルタ装置Aの接続と同様である。

【0034】私設網Cは、パケットフィルタ装置が存在しないため、ファイアウォールC106-3を介して公衆網と接続される。計算機Cは、ファイアウォールCに接続される。

【0035】また、パケットフィルタ装置計算機109は、パケットフィルタの機能を内蔵する計算機である。

【0036】なお、図1では直結経路107、ファイアウォール経路108とともに物理的な通信線のイメージで説明したが、ATM(Asynchronous Transfer Mode)のように一本の物理的な通信線の上に実現された論理的な通信線を経路と考えてもよい。

【0037】図2は、パケットフィルタ装置102の内部構成を示している。パケットフィルタ装置は、公衆網側に設置され、私設網から送信されるデータパケットに認証情報を付加し、又、公衆網から受信したデータパケットをファイアウォールに振り分けたり、付加された認証情報をチェックする装置である。

【0038】パケットフィルタ装置は、パケット転送手段201、パケット振り分け手段202、認証キー記憶手段203及び認証キー設定手段204を備える。また、パケットフィルタ装置は、直結経路107、ファイアウォール経路108、及び、公衆網103の三つの入出力回線を持っている。

【0039】パケット転送手段201は、直結経路107から受信した、計算機からのデータパケットに対して、認証情報を付加して公衆網103に送信し、また、ファイアウォール経路108から受信した、計算機からのデータパケットに対して、そのまま公衆網に送信する。

【0040】パケット振り分け手段202は、公衆網103から受信したデータパケットに対して、データパケットの特定位置にある、他のパケットフィルタ装置で付加された認証情報が付加されているか否かを判断して、認証情

報が付加されているデータパケットに対しては認証情報を検査し、正しい認証情報が付加されていれば、VPNにおけるデータパケットであるとして直結経路107に送信し、認証情報が付加されていないか、或いは、正しい認証情報でないデータパケットに対してはファイアウォール経路108に送信する。

【0041】認証キー記憶手段203は、認証情報を作成し、または、検査する時に参照する認証キーを記憶するメモリである。

【0042】認証キー設定手段204は、認証キーをパケットフィルタ装置の認証キー記憶手段203に設定するためのユーザインタフェースである。

【0043】本実施の形態では、私設網A及び私設網BはVPNを構成するため、認証キー設定手段により、パケットフィルタ装置A102-1及びパケットフィルタ装置B102-2の認証キー記憶手段203には共通の認証キーが設定されている。このように、VPNを構成する私設網に接続されるパケットフィルタ装置の認証キー記憶手段203には共通の認証キーを設定しておく。

【0044】つぎに、パケット転送手段201について詳細に説明する。図3は、パケット転送手段201の詳細な構成図を示している。図3において、パケット転送手段201は、経路判定手段301、認証情報作成手段302及び認証情報付加手段303を備える。

【0045】経路判定手段301は、直結経路107から受信したデータパケットか、或いは、ファイアウォール経路108から受信したデータパケットかを受信したポートにより判定し、直結経路から受信したデータパケットは、認証情報作成手段302及び認証情報付加手段303を経由させて公衆網103に送信し、ファイアウォール経路から受信したデータパケットは、そのまま公衆網に送信する。

【0046】認証情報作成手段302は、経路判定手段301から受け取ったデータパケットと、認証キー記憶手段203に記憶されている認証キーとから認証情報を作成する。本実施の形態では、暗号学で既に知られているハッシュ関数を用いて認証情報を作成する。

【0047】認証情報付加手段303は、認証情報作成手段302により作成された認証情報をデータパケットのあらかじめ定められた特定領域に付加する。

【0048】次に、図2に示すパケット振り分け手段202の構成を詳細に説明する。図4は、パケット振り分け手段202の詳細な構成図を示している。図4において、パケット振り分け手段202は、パケット判定手段401、認証情報検査手段402及び認証情報削除機能403を備える。

【0049】パケット判定手段401は、公衆網103から受信したデータパケットに対して特定領域に認証情報が付加されているか否かを判断し、認証情報が付加されているデータパケットは、認証情報検査手段402及び認証情報削除手段403を経由させて直結経路107に送信し、認証情報が付加されていない、或いは、正しい認証情報でな

いデータパケットは、ファイアウォール経路108に送信する。

【0050】認証情報検査手段402は、認証情報が正しいか否かを判定する。この場合、パケット判定手段401から受け取ったデータパケットと、認証キー記憶手段203に記憶されている認証キーとから新たに認証情報を作成し、データパケットに付加されている認証情報と一致するかいかなかを比較する。一致する場合、正しい認証情報と判定し、一致しない場合、正しい認証情報でないと判定する。

【0051】認証情報削除手段403は、正しい認証情報と判定されたデータパケットに挿入されている認証情報を削除する。

【0052】認証情報は、図5に示すデータパケットの特定の位置に挿入されている。図5は、データパケットのフォーマットを示している。データパケットは、送信先アドレス501、送信元アドレス502及びポート番号503が記述されたヘッダ1307-1と、データが記述されたペイロード1307-2とから構成される。本実施の形態では、認証情報を、例えば標準通信プロトコルInternet Protocol Version6(IPv6)で規定されているフォーマットに従って、データパケットに挿入する。IPv6では、ヘッダ1307-1とペイロード1307-2との間に任意の制御データ504を、制御データのサイズや種別を区別する制御ヘッダと共に挿入できるよう規定されており、これをを利用して認証情報用の制御ヘッダ505と共に認証情報506を挿入することで、認証情報の有無を判断できる。

【0053】次に、図6および図7を参照して本実施の形態における処理動作を説明する。図6および図7は、本実施の形態の構成における処理シーケンスを示している。ここでは、図1に示す私設網A101-1内の計算機A104-1が、VPNを構成する私設網B101-2内の計算機B104-2に通信を行う場合の手順について説明する。図6に、送信側の処理を示し、図7に受信側の処理を示す。

【0054】(1)計算機A101-1は、送信先アドレスを、私設網B101-2内の計算機B104-2にして、データパケットを送信する(図6に示す手順2000)。

【0055】(2)内部ルータA105-1は、データパケットのヘッダに記述された送信先アドレスをチェックする。送信先アドレスが、私設網A101-1とVPNを構成する私設網である場合、直結経路を使ってデータパケットをパケットフィルタ装置A102-1に送信する(手順2001)。その他の送信先アドレスの場合には、ファイアウォールに送信し、セキュリティチェックを行った後、ファイアウォール経路でデータパケットをパケットフィルタ装置Aに送信する(手順2002)。

【0056】(3)パケットフィルタ装置Aは、直結経路から受信したデータパケットに対して、図3に示す認証情報作成手段302及び認証情報付加手段303を用いて認証情報をデータパケットに付加し、公衆網103に送信す

る(手順2003)。ファイアウォール経路から受信したデータパケットに対しては、そのまま公衆網に送信する(手順2004)。

【0057】(4)受信側のパケットフィルタ装置B102-2は、公衆網103からデータパケットを受信する(図7に示す手順2005)。

【0058】(5)パケットフィルタ装置B102-2は、パケット判定手段401を用いてデータパケットに認証情報が付加されているか否かを判断する。認証情報が付加されている場合、認証情報検査手段402を用いて認証情報が正しいか否かを判断し、認証情報削除手段403を用いて認証情報を削除する(手順2006)。認証情報が正しい場合は、直結経路を経由して内部ルータB105-2にデータパケットを送信する(手順2007)。認証情報が付加されていない、或いは、正しい認証情報でない場合は、ファイアウォール経路を経由してファイアウォールB106-2にデータパケットを送信する(手順2008)。

【0059】(6)ファイアウォールB106-2は、ファイアウォール経路を経由して送信されたデータパケットに対して詳細なセキュリティチェックを行った後、内部ルータB105-2にデータパケットを送信する(手順2009)。

【0060】(7)計算機B104-2は、内部ルータBからデータパケットを受信する(手順2010)。

【0061】上述した図1～図7に示す実施の形態では、私設網間を公衆網に接続して通信する場合を説明している。携帯端末等を公衆網に直接接続するような場合には、携帯端末にパケットフィルタ装置と同等の機能をソフトウェア、或いは、ハードウェアとして提供することで本実施の形態を実現することができる。すなわち、上述した機能は、ソフトウエアにより実現することができる。

【0062】パケットフィルタ装置のハードウエア構成を図14に示す。図14において、パケットフィルタ装置は、公衆網に接続される公衆網接続部1450と、私設網に直接接続される私設網接続部1410と、ファイアウォールに接続されるファイアウォール接続部1420と、処理を行うCPU1430と、公衆網接続部1450で受信したパケットがあらかじめ定めた送信元から送信されたパケット(認証情報が付加されたパケット)であるかないかを判断し、あらかじめ定めた送信元からのパケットであれば、私設網接続部1410から当該データパケットを送信し、あらかじめ定めた送信元からのパケットでなければファイアウォール接続部1420から当該データパケットを送信させるためのプログラムを記憶するメモリ1440とを有する。さらに、メモリ1440は、私設網接続部1410で受信したパケットにあらかじめ定めた送信元情報(認証情報)を付加して公衆網接続部1450から当該パケットを送信し、ファイアウォール接続部1420で受信したパケットはそのまま公衆網接続部1450から送信させるプログラムを備

える。

【0063】本実施の形態によれば、パケットフィルタ装置により、VPNのサービスを網側で提供することができる。また、VPNを構成する私設網間の通信は、セキュリティを守りつつ、リアルタイムデータの転送を実現することができる。VPN以外の通信は、ファイアウォールによる細やかなセキュリティが実現できる。

【0064】つぎに、第2の実施の形態について説明する。

10 【0065】第1の実施の形態では、各私設網が一つのVPNグループにのみ属する例を考えてきた。しかし、一つの私設網が、複数のVPNグループに属する場合も考えられる。例えば、図1に示す私設網Aと私設網Bとで第1のグループを作り、私設網Aと私設網Cで別の第2のグループを作るような場合である。この場合、グループ毎に異なる認証キーを持つことで、どのグループに属するデータパケットかを区別することができる。第2の実施の形態では、第1の実施の形態と同様な構成で、認証キーをVPNグループごとに設けて、各自の認証を行う。

20 【0066】第2の実施の形態における認証キーについて図8を参照して説明する。図8は、認証キー記憶手段203として単に一つの認証キーを記憶するのではなく、複数の認証キーを管理する方法について示した説明図である。本実施の形態では、VPNグループに属する私設網のアドレス群と、認証キーとを対にして記憶する。対の数は、私設網が属するVPNグループの数に一致する。

【0067】認証情報作成手段302では、ヘッダ1307-1に記述された送信先アドレスから、また認証情報検査手段402では、ヘッダ1307-1に記述された送信元アドレスからVPNグループに対応した認証キーを検索して認証情報の作成、或いは、検査を行う。

【0068】本実施の形態により、異なる認証キーを用いることでデータパケットがどのVPNグループに属するかを判別することが可能となる。

【0069】次に、第3の実施の形態を説明する。第3の実施の形態では、VPNグループごとに、私設網101及びパケットフィルタ装置102を接続させる直結経路107を設ける場合について、図9を参照して説明する。

40 【0070】図9は、複数のVPNグループに対応した認証キー管理方法について示した説明図である。

【0071】図9において、認証キー記憶手段203は、直結経路の番号に対応して認証キーを記憶する。内部ルータ105は、グループに対応した直結経路にデータパケットを送信する。認証情報作成手段302は、認証キー記憶手段203の情報を使ってデータパケットが送信された直結経路のポート番号から認証キーを検索し、認証情報を作成する。認証情報検査手段402は、認証キー記憶手段の情報を使って各直結経路に対応した認証キーから順に、或いは、並列に認証情報を検査し、一致する認証情報を見つける。パケット判定手段401は、対応する直結

経路を求め、データパケットを振り分ける。

【0072】本実施の形態により、直結経路107と認証キーとは一対一に対応する。よって、パケット転送手段201は、認証キーを高速に検索できる。

【0073】次に第4の実施の形態について説明する。第4の実施の形態では、認証キー記憶手段203に記憶される認証キーを通信開始時に設定する場合について説明する。図10は、認証キー記憶手段203に記憶される認証キーを通信開始時に設定する場合の構成図である。本実施の形態では、認証サーバー1001を公衆網103上に設置する。認証サーバー1001は、公衆網103に接続された全てのパケットフィルタ装置102が所有する認証キーを記憶した記憶手段1010と、パケットフィルタ装置102を認証するパケットフィルタ装置認証手段1011と、認証キーをパケットフィルタ装置102に送信する認証キー送信手段1012とを備える。

【0074】パケットフィルタ装置A102-1の認証キー設定手段204-1は、認証キーを設定するために、認証サーバー1001と以下の手続きを行う。

【0075】(1) 公衆網103との最初の通信を開始する時に認証サーバー1001と接続させる。パケットフィルタ装置A102-1の認証キー設定手段204-1は、あらかじめパスワードを受け付けておく。

【0076】(2) パケットフィルタ装置認証手段1011は、あらかじめ定めたパスワードを交換することでパケットフィルタ装置A102-1を認証する。

【0077】(3) 認証キー送信手段1012は、記憶手段1010から認証キーを取り出して、パケットフィルタ装置A102-1に送信する。

【0078】(4) 受信した認証キーを認証キー記憶手段203-1に設定する。

【0079】パケットフィルタ装置B102-2も同様の手続きを行い、認証キーを設定することができる。

【0080】本実施の形態により、認証キーの一元管理が可能となる。よって、認証キーの変更を行う場合、認証サーバー1001上の一力所で行うことができる。

【0081】つぎに、第5の実施の形態を説明する。第3の実施の形態では、公衆網103とパケットフィルタ装置102とを一つの経路で接続させた。しかし本実施の形態では、図11に示す様に、複数の直結経路107及び一つのファイアウォール経路108に一対一で対応した経路で公衆網と、パケットフィルタ装置とを接続させる。すなわち、VPNごとに、直結経路107および公衆網とを設けておく。

【0082】パケット転送手段201は、直結経路を介して受信したデータパケットに対しては、直結経路に対応した認証情報を付加して、私設網側の直結経路に対応する公衆網側の経路に送信する。ファイアウォール経路を介して受信したデータパケットに対しては、そのまま私設網側のファイアウォール経路に対応する公衆網側の経

路に送信する。

【0083】パケット振り分け手段202は、公衆網から受信したデータパケットをチェックし、正しい認証情報が付加されているデータパケットは、認証情報を取り除いて対応する直結経路に送信する。正しい認証情報が付加されていないデータパケットは、ファイアウォール経路に送信する。

【0084】本実施の形態により、パケット振り分け手段202は、経路により、VPNのグループの判別が容易になる。よって、パケット振り分け手段の高速化が可能となる。

【0085】上述した実施の形態によれば、パケットフィルタ装置が付加する認証情報は、アプリケーションポートコルに係わらず一定であるため、ハードウェアによる実現が可能であり、高速なインターネットVPNを実現できる。更に、私設網内のあるVVサーバーへのアクセスを許す場合や、逆に私設網から公衆網上のVVサーバーをアクセスする際等、VPN外の情報処理装置へのアクセスはファイアウォールを経由して行えるので、速度は直結経路より落ちるが、細やかなセキュリティの実現が可能である。

【0086】

【発明の効果】本発明によれば、VPNを構成する私設網間の通信は、セキュアで且つリアルタイムデータの転送を可能とし、VPN以外の通信は、ファイアウォールによる細やかなセキュリティが実現できる。

【図面の簡単な説明】

【図1】本発明の実施の形態におけるシステム構成図である。

【図2】本発明の実施の形態におけるパケットフィルタ装置の内部構成図である。

【図3】本発明の実施の形態におけるパケット転送手段の詳細を示す説明図である。

【図4】本発明の実施の形態におけるパケット振り分け手段の詳細を示す説明図である。

【図5】認証情報を付加したデータパケットの説明図である。

【図6】本発明の実施の形態における送信側の処理動作を示すシーケンス図である。

【図7】本発明の実施の形態における受信側の処理動作を示すシーケンス図である。

【図8】本発明の実施の形態における認証キー記憶手段の他の説明図である。

【図9】本発明の実施の形態における認証キー記憶手段の他の説明図である。

【図10】本発明の実施の形態におけるシステム構成に認証サーバーを追加した構成図である。

【図11】パケットフィルタ装置の他の構成図である。

【図12】ファイアウォールを用いた従来技術を示す構成図である。

【図13】従来技術におけるファイアウォールの内部構成図である。

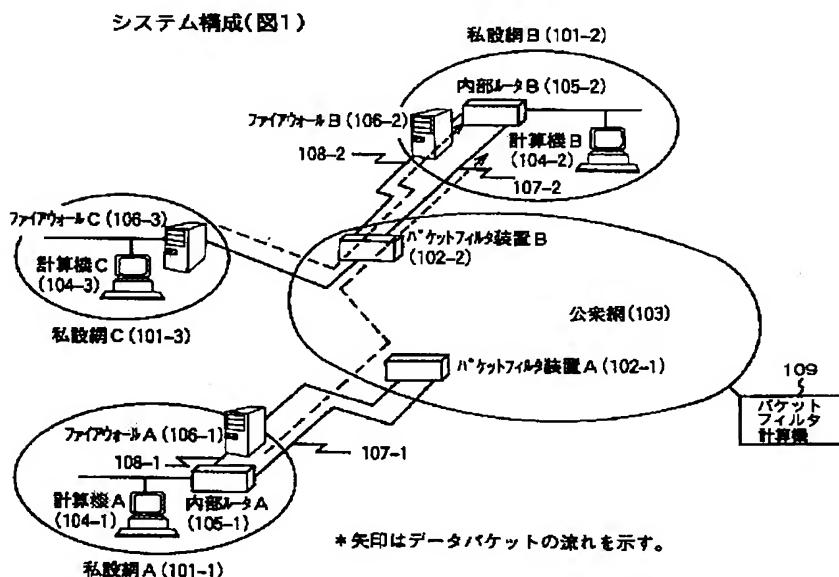
【図14】パケットフィルタ装置の構成図。

【符号の説明】

101...私設網、102...パケットフィルタ装置、103...公衆網、104...計算機、105...内部ルータ、106...ファイアウォール、107...直結経路、108...ファイアウォール経路、201...パケット転送手段、202...パケット振り分け手段、203...認証キー記憶手段、204...認証キー設定手段、301...経路判定手段、302...認証情報作成手段、303...認証情報付加手段、401...パケット判定手段、402...認証情報検

査手段、403...認証情報削除手段、501...送信先アドレス、502...送信元アドレス、503...ポート番号、504...制御データ、505...制御ヘッダ、506...認証情報、507...データ、1001...認証サーバ、1010...記憶手段、1011...パケットフィルタ装置認証手段、1012...認証キー送信手段、1301...入出力手段、1302...暗号化手段、1303...コネクション管理手段、1304...アプリケーション管理手段、1305...コネクション管理テーブルA、1306...コネクション管理テーブルB、1307...データパケット。

【図1】



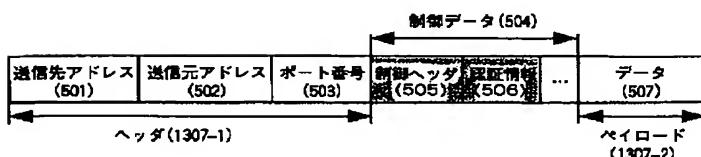
【図8】

認証キー記憶手段の変更例1(図8)

認証キー記憶手段 (203)	認証キー情報
VPNグループAの宛先アドレス群	認証キーA
VPNグループBの宛先アドレス群	認証キーB
VPNグループCの宛先アドレス群	認証キーC
⋮	⋮

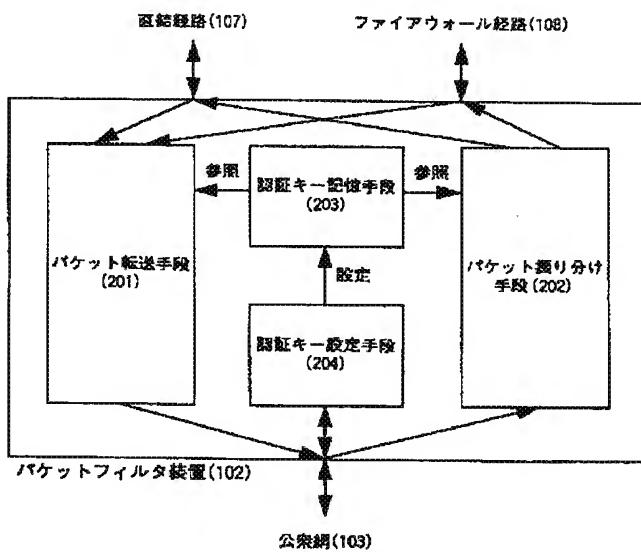
【図5】

データパケット(図5)



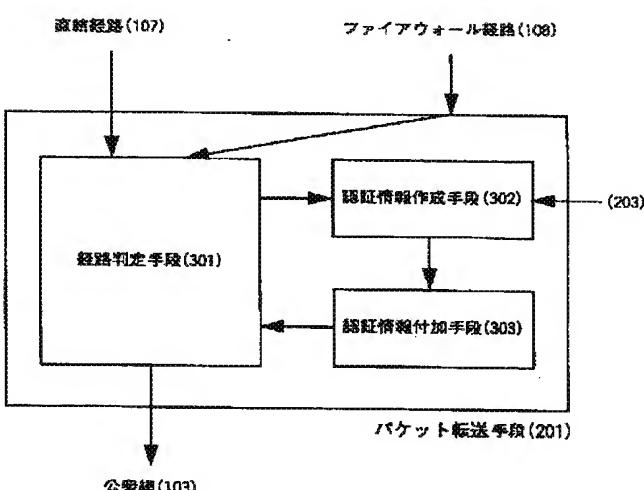
【図2】

パケットフィルタ装置(図2)



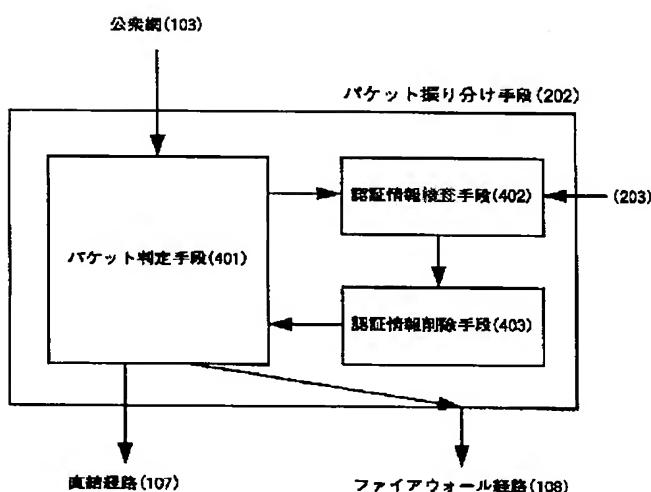
【図3】

パケット転送手段(図3)



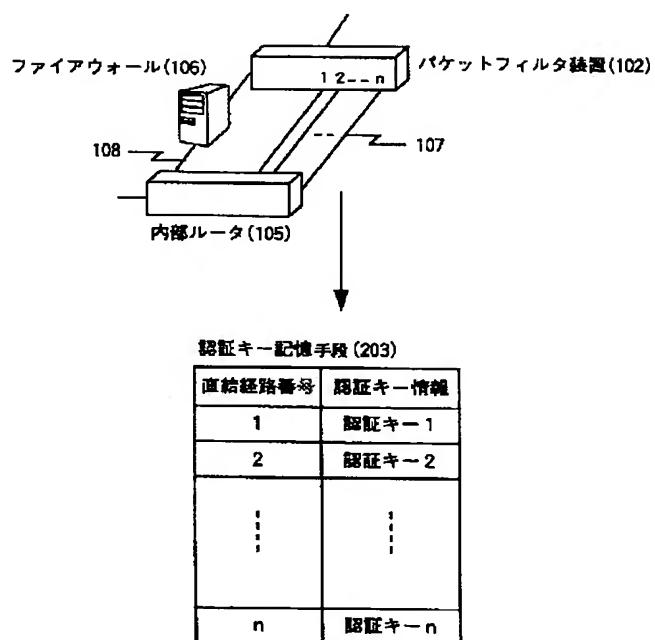
【図4】

パケット振り分け手段(図4)



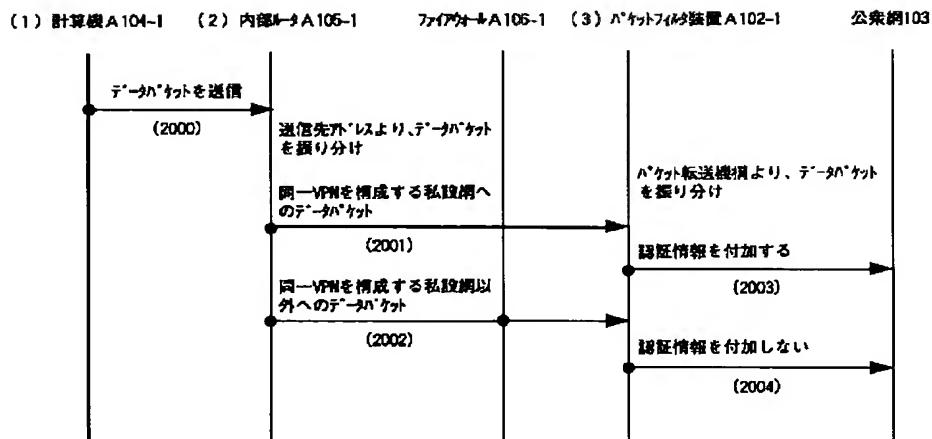
【図9】

認証キー記憶手段の変形例2(図9)



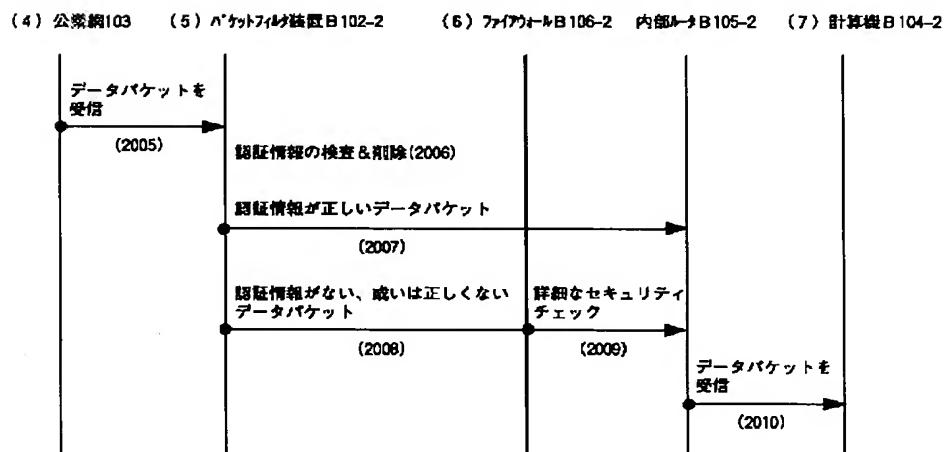
【図6】

処理の流れ(送信側) (図6)



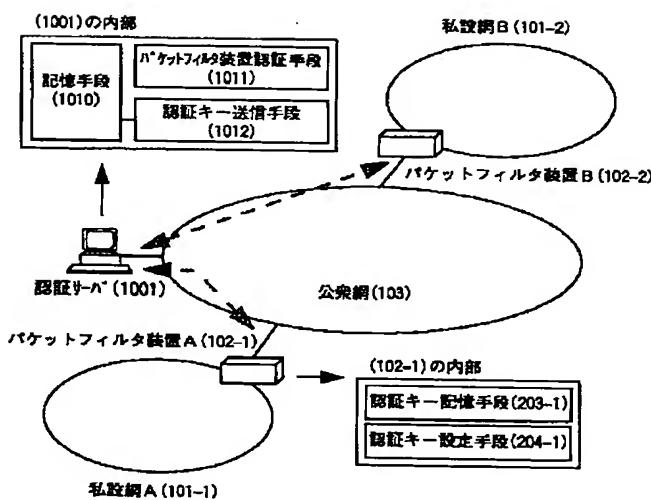
【図7】

処理の流れ(受信側) (図7)



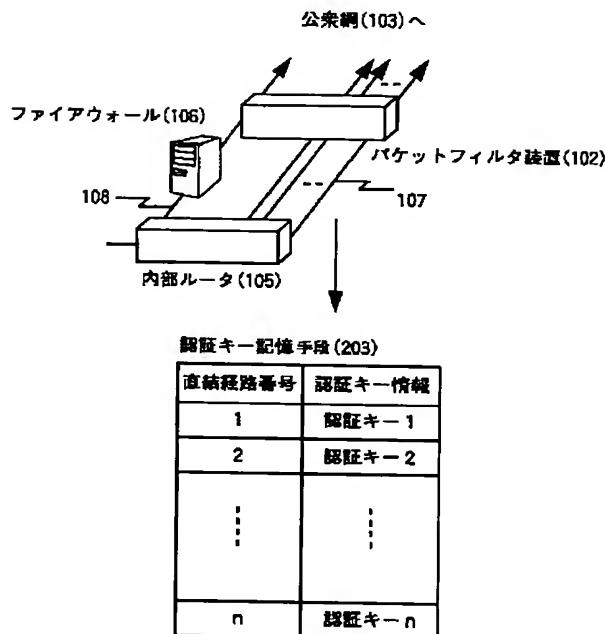
【図10】

認証サーバ(図10)



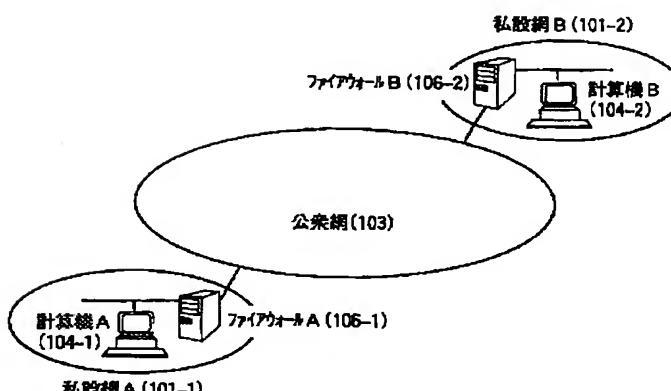
【図11】

パケットフィルタ装置の変形例(図11)



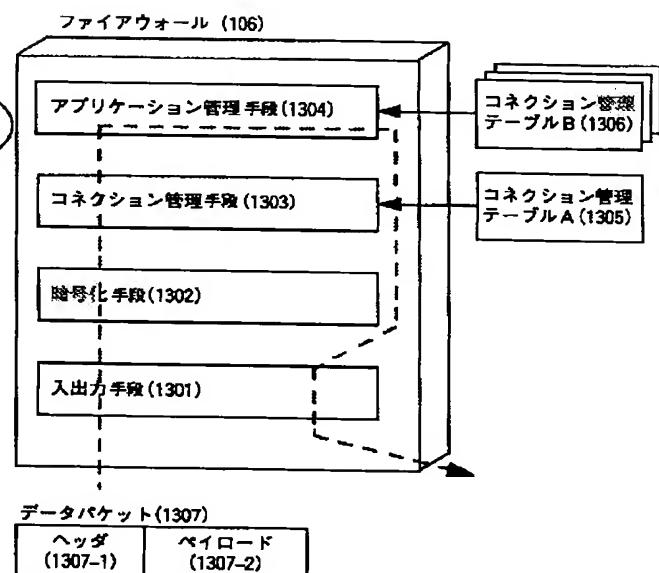
【図12】

従来技術(図12)



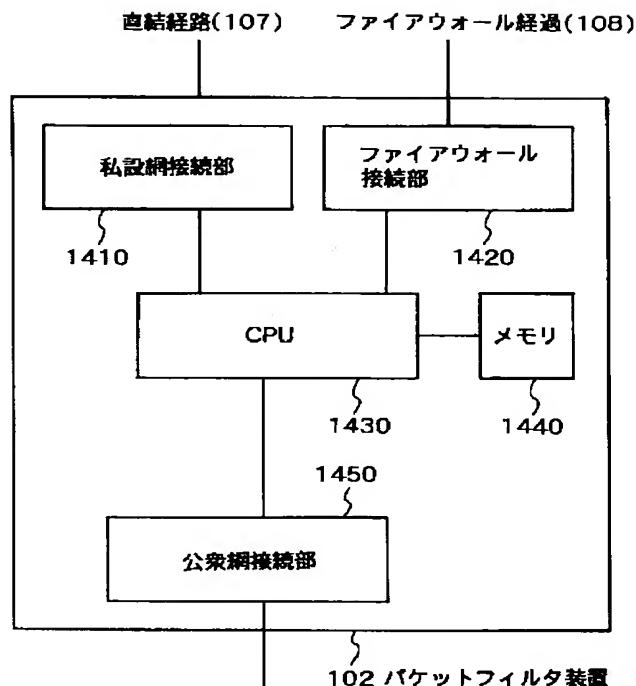
【図13】

ファイアウォールの内部構成(図13)



【図14】

図14



フロントページの続き

(72) 発明者 太田 正孝
神奈川県横浜市戸塚区戸塚町216番地 株
式会社日立製作所情報通信事業部内